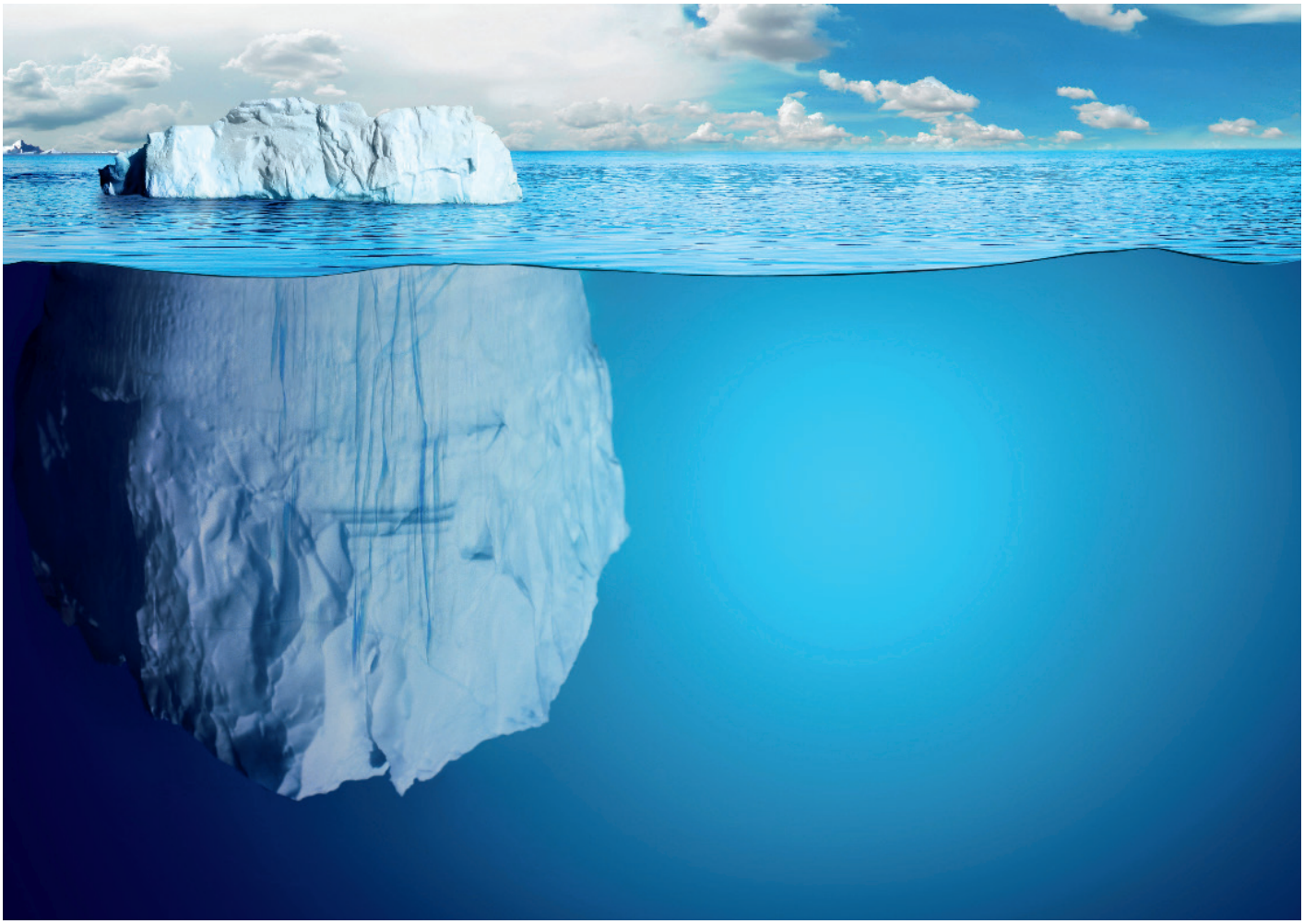
Deloitte.



Internal Audit Insights
High impact areas of focus

Die Rolle der Internen Revision hat sich in den vergangenen Jahren stark gewandelt.

Neue Risiken und das gestiegene Sicherheitsbedürfnis des Managements und der Aufsichtsorgane haben die Anforderungen an die interne Überwachung erhöht und die Rolle der Internen Revision verändert.

Um den wachsenden Anforderungen gerecht zu werden, muss Internal Audit das ganze Spektrum an Themen rund um Governance, Risk und Compliance im Blick haben und sich der modernsten Techniken und Tools bedienen.

In der Ausgabe 2016 der Serie „Internal Audit Insights" geben wir einen Überblick über neueste Entwicklungen in diesem Bereich.

International Professional Practices Framework

Das Institute of International Auditors (IIA) gab im Juli 2015 eine aktualisierte Version des International Professional Practices Framework (IPPF) heraus, um die sich ändernde Rolle von Internal Audit zu berücksichtigen – die erste größere Überarbeitung seit 1999. Die Definition, der Verhaltenskodex und die Berufsstandards sind gleich geblieben, wohingegen die Berufsgrundlagen einen neuen Leitspruch und neue Prinzipien für die Berufspraxis enthalten. Der Leitspruch – „den Wert einer Organisation durch risikoorientierte und objektive Prüfung, Beratung und Einblicke zu erhöhen und zu schützen" – gibt das Ziel der Internal-Audit-Funktion vor. Damit wird die Mission und Rolle der Funktion im Rahmen der Unternehmensführung ebenso berücksichtigt wie die Notwendigkeit, die wichtigsten Stakeholder zu beraten und Einblicke zu gewähren. Aktuell konzentrieren sich viele Internal-Audit-Einheiten nach wie vor stark auf die Sicherheit etablierter Kontrollen, die Ordnungsmäßigkeit der Prozesse und z.B. die Einhaltung des Sarbanes-Oxley (SOX) Act sowie anderer Vorschriften.

Empfohlene Maßnahmen

Um die in den IPPF festgelegte Mission zu erfüllen, sollten die Internal-Audit-Verantwortlichen beurteilen, wie sie derzeit positioniert sind und ob Veränderungen nötig sind, um neue Risikofelder abzudecken. Überprüfen Sie regelmäßig, wie Ihre Funktion die Mission und die Hauptgrundsätze von Internal Audit erfüllt. Schauen Sie sich die Qualitätssicherung und Verbesserungen an: Gibt es ein Programm? Wie nachhaltig ist es? Wie werden Qualität und Verbesserungen gemessen? Beurteilen Sie Prüfungspläne auch dahingehend, welcher Prozentsatz der Mittel für die Ordnungsmäßigkeit statt für beratende oder wertschöpfende Tätigkeiten eingesetzt wird. Nutzen Sie die IPPF, um eine Diskussion über den zusätzlichen Wertbeitrag einer Neuausrichtung von Internal Audit anzuregen. Dies kann möglicherweise eine Schulung der Geschäftsführung und/oder des Aufsichtsrats erfordern, insbesondere dann, wenn „althergebrachte" Vorstellungen zur Rolle und Aktivität von Internal Audit bestehen. Achten Sie außerdem auf die sich entwickelnden Leitlinien des IIA und beurteilen Sie die Internal-Audit-Programme anhand der IIA-Standards entweder mittels einer internen Abweichungsanalyse, einer externen Prüfung oder einer Selbsteinschätzung mit nachträglicher unabhängiger, externer Validierung.

… „den Wert einer Organisation durch risikoorientierte und objektive Prüfung, Beratung und Einblicke zu erhöhen und zu schützen" …

Dynamische Prüfungsplanung

Eine dynamische Prüfungsplanung kennzeichnet sich durch eine regelmäßige oder kontinuierliche Anwendung qualitativer und quantitativer Methoden, um Problemfelder eines Unternehmens zu identifizieren und die Ressourcen auf Schlüsselrisiken auszurichten. Im Vergleich zu statischen oder turnusmäßigen Prüfungsplänen stellt dies ein großer Schritt vorwärts dar. Risiken und Chancen treten plötzlich auf und das Unternehmen muss sich damit befassen. Deshalb bietet die dynamische Prüfungsplanung einen flexiblen, anpassungsfähigen Ansatz, bei dem Selbsteinschätzungen, Datenanalysen und kontinuierliche Überwachungsmaßnahmen („Continuous Auditing") die jährlich risikobasierten Einschätzungen ergänzen. Eine dynamische Prüfungsplanung befähigt Internal Audit zu dessen Mission, Risiken zu antizipieren und wirksam abzusichern. Auditoren sind dadurch in der Lage, das Management im Hinblick auf Risiken kompetent zu beraten und Maßnahmenempfehlungen zur Risikominderung zu geben.

Empfohlene Maßnahmen

Es ist notwendig, zu erkennen, dass eine dynamische Prüfungsplanung Auditoren braucht, die über die Themen Strategie, Geschäft, Betrieb und Risiken ebenso informiert sind wie über Finanzprozesse, -systeme und -kontrollen. Außerdem erfordert sie eine Flexibilität, um problemlos mit Planungsänderungen umgehen und rasch auf neue Anforderungen reagieren zu können. Internal Audit kann beispielsweise bei einer geplanten Akquisition helfen, indem Risiken und Grenzen der Wertschöpfung aufgezeigt werden. Als Beispiel seien Probleme beim Umgang mit Vorschriften oder bei der Integration von Systemen und Kontrollen genannt. Darüber hinaus können künstliche Intelligenz und Techniken zur Risikomessung ein dynamisches Internal Audit wirkungsvoll unterstützen.

Internal Audit Analytics

Internal Audits, die ausschließlich auf vergangenheitsbezogene Stichprobenprüfungen abstellen, können die Anforderungen der Stakeholder insbesondere hinsichtlich neu auftretender Risiken („Emerging Risks"), strategischer Fragestellungen sowie der Verbesserung der Leistungsfähigkeit kaum erfüllen. Daher wächst der Bedarf an Analysetools, die einerseits leistungsfähiger geworden sind und andererseits selten ein technisches Spezialwissen bei den Anwendern voraussetzen. Massendatenanalysen über alle Bestellungen, Rechnungen und Zahlungen einer Geschäftseinheit in einem bestimmten Zeitraum bieten eine höhere Chance, Unregelmäßigkeiten, Kontrollschwächen und Betrugsfälle aufzudecken, als zufallsbasierte Stichproben. Außerdem hat der Prüfer die Möglichkeit, sich bei auffälligen Transaktionen die dahinterstehenden Daten im Detail anzeigen zu lassen („Drill down"). Diese Datenanalysen können große Datenvolumina auf „Red Flags" bzw. Risikoindikatoren analysieren und zu der Aufdeckung von Risiken beitragen. Allerdings nutzen viele Internal-Audit-Abteilungen diese Methoden nur unzureichend, da sie häufig den Nutzen nicht erkennen, die Komplexität überschätzen oder möglicherweise veränderungsresistent sind. Diejenigen, die inzwischen Analysetools verwenden, sind häufig in der Lage, die Qualität, Effizienz und Effektivität ihrer Arbeit deutlich zu steigern und zusätzlichen Mehrwert für das Unternehmen zu generieren.

Empfohlene Maßnahmen

Beginnen Sie damit, ein handelsübliches Analysetool für diejenigen Datensätze zu verwenden, bei denen sich die Investition rasch lohnen wird, wie beispielsweise Spesenabrechnungen oder Lieferantenkosten. Analysieren Sie die Ursachen für Abweichungen. Wurden Richtlinien falsch verstanden, bewusst umgangen oder handelt es sich um Kontrollversagen? Erarbeiten Sie Lösungen, um einen Mittelabfluss zukünftig zu vermeiden und verlorenes Geld zurückzubekommen.
Es ist davon auszugehen, dass je nach Branche die Aufsichtsbehörden Bereiche definieren werden (wie im Bankwesen bereits geschehen), die datenanalytisch überwacht sein müssen. Internal Audit kann hierbei eine aktive Rolle spielen und die erste bzw. zweite Verteidigungslinie des Unternehmens verstärken.

Es wächst der Bedarf an Analysetools, die einerseits leistungsfähiger geworden sind und andererseits selten ein technisches Spezialwissen bei den Anwendern voraussetzen.

Cybersicherheit

Entscheidend für die Effektivität von Cyber Security Audits sind die verschiedenen Möglichkeiten, Cyberrisiken zu definieren und entsprechende Vorkehrungen zu treffen. Zu viele Audits konzentrieren sich auf einzelne, ausgewählte Aspekte – z.B. Internetsicherheit, Datenzugriff oder die Firewall – und das Ergebnis wird dann als Cyber Security Audit präsentiert. Dieser Ansatz bietet zwar ein gewisses Maß an Sicherheit, deckt aber möglicherweise nicht auf, in welchem Umfang die Cybersicherheit des Unternehmens tatsächlich bedroht ist. Diese sollte umfassend definiert sein und auf Standards und Rahmenwerken wie z.B. BSI, ISO, COSO und ITIL basieren. Sie sollte sämtliche immateriellen Vermögenswerte sowie Prozesse und Systeme berücksichtigen, die Daten generieren, speichern, analysieren und transportieren. Hierzu gehören auch E-Mails, Textnachrichten, soziale Medien, Massendaten sowie das Internet. Aufgrund der steigenden Bedrohung sollte Internal Audit die Aufmerksamkeit und Robustheit des Unternehmens hinsichtlich neuer Cyberbedrohungen regelmäßig beurteilen und Verbesserungen anstoßen.

Empfohlene Maßnahmen

Als dritte Verteidigungslinie sollte Internal Audit eine Beurteilung der Cyberbedrohung anhand eines verlässlichen Ansatzes durchführen, welcher Sicherheit, Wachsamkeit (Fähigkeit, Bedrohungen zu erkennen) und Widerstandsfähigkeit (Reaktion ohne wesentliche Beeinträchtigung des Geschäftsbetriebs) berücksichtigt. Internal Audit sollte dabei die Bedrohungslage berücksichtigen (wer könnte der Angreifer sein, warum könnte der Angriff erfolgen und was könnte das Ziel des Angriffs sein).

Eine weiterführende Prüfung sollte sich mit der Angemessenheit der durch die erste (operative Ebene) und der zweite (prozessabhängige Beratung und Überwachung) Verteidigungslinie ergriffenen Maßnahmen angesichts der bestehenden und antizipierten Cyberbedrohungen befassen.

Je nach Unternehmen könnten zu den Hochrisikobereichen u.a. der Datenschutz, das Lieferantenmanagement, das „Cyber Incident"-Management sowie die Robustheit gegenüber Angriffen, Störungen und Veränderungen gehören. Diese iterative und häufig über mehrere Jahre andauernde Initiative erfordert sowohl einen programmatischen als auch einen nach Prioritäten ausgerichteten Ansatz.

Cyber Security Audits erfordern eine laufende Förderung und Weiterbildung der Internal Auditors und eine enge Zusammenarbeit mit den Mitarbeitern der IT, der Unternehmenssicherheit, der Geschäftsbereiche sowie des Risikomanagements.

Data Governance

Die meisten Organisationen brauchen in irgendeiner Art und Weise eine Data Governance, d.h. einen Ordnungsrahmen für die Steuerung und Überwachung von Daten. Besonderheiten sind unternehmens- und branchenabhängig, grundsätzlich umfasst Data Governance Richtlinien und Verfahren bezüglich der Verantwortlichkeit für die Daten sowie der Nutzungszwecke, der Verlässlichkeit und der Richtigkeit der Daten. Weitere Themen sind die Handhabung der Daten und Sicherungsmaßnahmen, um Verlust oder Diebstahl zu verhindern oder auch für eine vorschriftsgemäße Datenvernichtung zu sorgen. Risiken treten üblicherweise im Zusammenhang mit Datenschutz, regulatorischen Anforderungen und der Unternehmensreputation auf, wobei der potenzielle Verlust oder Diebstahl von Kundendaten eine häufig geäußerte Sorge ist. Internal Audit sollte seine Data-Governance-Schwerpunkte an den Bedürfnissen des Unternehmens hinsichtlich der Data Governance abstimmen. Beispielsweise haben verschiedene Branchen (wie z.B. Finanzdienstleister oder Pharmaunternehmen) unterschiedliche Anforderungen an die Data Governance und benötigen daher auch unterschiedliche Data-Governance-Ansätze.

Empfohlene Maßnahmen

Konzentrieren Sie sich zuerst auf die sensibelsten Daten und diejenigen, die einem vergleichsweise hohen Risiko ausgesetzt sind. Überprüfen Sie Richtlinien und Verfahren entlang des gesamten Datenlebenszyklus. Dies umschließt Erfassung, Speicherung, Transport und Vernichtung von Daten sowie die Steuerung des Zugriffs und die Sicherstellung der Datenqualität. Die Umsetzung von Richtlinien und Verfahren sollte nicht außer Betracht gelassen werden. Bieten Sie den Geschäftseinheiten, die keine oder nur rudimentäre Richtlinien und Verfahren haben, Lösungen und Ratschläge. Vermeiden Sie eine reine Beurteilung der Datenqualität und konzentrieren Sie sich stattdessen auf die Prozesse und Kontrollen, welche die gewünschte oder erforderliche Datenqualität erzeugen oder schützen.

Konzentrieren Sie sich zuerst auf die sensibelsten Daten und diejenigen, die einem vergleichsweise hohen Risiko ausgesetzt sind.

Key Performance Indikatoren

Das Management verwendet nicht-finanzielle Key Performance Indikatoren (KPIs), um Kundenbeziehungen, Produktqualität, Nachhaltigkeit und allgemein Chancen und Risiken zu messen, zu steuern und zu überwachen. Allerdings sind die Prozesse, Systeme und Kontrollen für diese Leistungsindikatoren i.d.R. deutlich weniger entwickelt als diejenigen für Finanzdaten. Deshalb lassen sich Prüfungskompetenzen und -methoden durchaus auch auf nicht-finanzielle KPIs anwenden. Internal Audit kann diese nutzen, um Prozesse, Systeme und Kontrollen zu beurteilen und Verbesserungen abzuleiten. Die Existenz und Qualität wesentlicher Leistungsindikatoren ist ein zunehmend wichtiger Aspekt für die externe Berichterstattung und ermöglicht der Geschäftsführung, öffentliche Aussagen wirkungsvoll zu untermauern. Beispielsweise erfordern Berichte zu Energie- oder Wasserverbrauch und Arbeitspraktiken sowie Aussagen zu Kundendienst und Produktqualität präzise und verlässliche Leistungsindikatoren. Internal Audit ist in einer guten Position, Anstöße zu geben und Mehrwert zu generieren.

Empfohlene Maßnahmen

Überprüfen Sie die Existenz und Qualität erfolgskritischer Leistungsindikatoren. Achten Sie auf diejenigen, die in Nachhaltigkeitsberichten verwendet werden, bei Behörden eingereicht werden oder marktseitige Relevanz haben, wie beispielsweise Messzahlen zu Servicequalität, -verfügbarkeit und pünktlicher Lieferung. Analysieren Sie die Logik der Leistungsindikatoren und Zusammenhänge. Gibt es Lücken oder Inkonsistenzen? Wenden Sie dann die Prüfungskompetenz auf die zugrunde liegenden Prozesse und Systeme an. Die interne Prüfung sollte in einem ersten Schritt verifizieren, ob das Management sich in Bezug auf das, was gemessen werden soll, an den richtigen Leistungsindikatoren orientiert und ob die zugrunde liegenden Prozesse richtig konzipiert, implementiert und überwacht sind. Die Interne Revision ist damit in der Lage, die Eignung und Verlässlichkeit der Leistungsindikatoren zu beurteilen und Verbesserungspotenziale in Bezug auf die Daten und Prozesse abzuleiten.

Planung Krisenmanagement

Globalisierung und Virtualisierung des Geschäftslebens führen dazu, dass jede Krise weitreichende Folgen haben kann, während soziale Medien das Reputationsrisiko eines Unternehmens deutlich erhöhen. Trotzdem denken viele Internal-Audit-Einheiten bei der Vorbereitung auf Krisen vor allem an Geschäftskontinuität, Reaktionen im Notfall und Notfallwiederherstellung. Heutzutage muss die Planung des Krisenmanagements diese Elemente in einen umfassenden Reaktionsplan integrieren. Dieser muss auch die interne und externe Kommunikation einbinden und, soweit erforderlich, die weltweite Koordination, damit das Management jeder Krise immer einen Schritt voraus ist und um alle Stakeholder zu berücksichtigen.

Empfohlene Maßnahmen

Bei der Prüfungsplanung kann Internal Audit feststellen, ob das Management potenzielle Krisen und deren voraussichtliche Auswirkungen in vollem Umfang berücksichtigt hat. Die Folgen einer Krise – einer Naturkatastrophe oder durch Menschen verursachten Krise, einer physischen oder virtuellen, einer lokalen oder weit entfernten Krise – können Betrieb, Mitarbeiter, Lieferketten, Werke, Anlagen sowie IT und Daten beeinträchtigen. Prüfungspläne sollten deshalb sicherstellen, dass Krisenszenarien holistisch und integriert betrachtet werden und sämtliche Auswirkungen berücksichtigen. In jedem Prüfungszyklus kann man sich dann auf zwei oder drei Bereiche fokussieren, um die Detailtiefe, die Reaktionsfähigkeit sowie die Integration von Plänen zu beurteilen. In Unternehmen mit weniger ausgereiften Ansätzen für das Krisenmanagement kann sich Internal Audit mehr auf die Beratung als auf die Prüfung konzentrieren und Orientierungshilfe bieten.

Die Folgen einer Krise können Betrieb, Mitarbeiter, Lieferketten, Werke, Anlagen sowie IT und Daten beeinträchtigen.

Lieferantenmanagement

Die Geschäftsbeziehungen mit Lieferanten werden immer komplexer und bergen neue Risiken, die selten wirkungsvoll auslagert oder versichert werden können. Überwachung und Steuerung solch externer Risiken sind häufig auf verschiedene Geschäftseinheiten und Fachabteilungen verteilt, sodass eine Gesamtsicht über vertraglich fixierte Geschäftsbeziehungen häufig fehlt.
Vielfach sind Geschäftsbeziehungen von Vertrauen geprägt und die Überwachung der Vertragserfüllung unzureichend organisiert. Ein aktiver, präventiver und überwachter Ansatz im Lieferantenmanagement ist selten vorzufinden.
In einem optimierten Zustand werden Verträge und Leistungskennzahlen (KPIs) von Lieferanten mit dem Ziel überprüft, den gesamten Wert aus den Lieferantenverträgen zu erschließen. Gegenüber bestimmten Lieferantengruppen empfiehlt es sich, Prüfungsrechte zu vereinbaren und die Vertrags-Compliance regelmäßig zu überwachen (Third Party Audits).
Jedoch ist zu beachten, dass diejenigen, die derartige Prüfungen durchführen, über die erforderliche Kompetenz verfügen, spezielle Geschäftsmodelle und komplexe Vertragsbestimmungen zu untersuchen.

Empfohlene Maßnahmen
Internal Audit sollte frühzeitig bei komplexen und strategischen Lieferantenentscheidungen sowie der vertraglichen Fixierung von kritischen Geschäftsbeziehungen einbezogen werden. Wenn die Vertragsparteien gleich am Anfang Klarheit schaffen und die Chancen und Risiken erfassen, unterstützt das die Geschäftsbeziehung und Zusammenarbeit nachhaltig. Viele Lieferanten schätzen einen frühen Hinweis auf Fehler oder Regelungslücken, statt am Ende mit langwierigen Auseinandersetzungen beschäftigt zu sein. In der Anlaufphase der Geschäftsbeziehung können Datenanalysen die Prüfung von Leistungsindikatoren unterstützen sowie Fehler und Anomalien aufdecken. Ein pragmatischer Internal-Audit-Ansatz fördert die Akzeptanz und schafft Mehrwert für das Unternehmen.

Compliance Management

Compliance ist aktueller denn je. Obwohl sich in den letzten Jahren anerkannte Standards entwickelt haben, stellt sich für Vorstand und Aufsichtsrat häufig noch die Frage: „Tun wir genug im Bereich Compliance, um persönliche Haftungsrisiken sowie mögliche Rechtsfolgen für das Unternehmen wirksam zu vermeiden?“ Kein Unternehmen ist zu 100 Prozent immun gegenüber Fehlverhalten, daher sollte jede Firma entsprechend Vorsorge treffen. Dabei ist es wichtig, zunächst das Risiko für das Unternehmen einzuschätzen, um angemessene Maßnahmen treffen und auf mögliche Non-Compliance reagieren zu können. Gab es bereits Vorfälle? Wie sind die Governance und das Kontrollumfeld ausgestaltet? Ist das Geschäftsmodell anfällig für Verstöße? Gibt es landesspezifische Unterschiede? Drohen Bußgelder, Rufschädigung oder Geschäftsbeeinträchtigungen? Viele Fragen gilt es im Vorfeld zu beantworten, um angemessene und effektive Maßnahmen der Vorbeugung, Aufdeckung und Reaktion auf Non-Compliance zu treffen. Die Mehrzahl der Compliance-Vorfälle wird mittlerweile durch Hinweisgeber aufgedeckt, aber auch interne und externe Prüfungen spielen eine wichtige Rolle bei der Erkennung und Aufklärung von Verstößen. Der Übergang vom Internal Audit zur Investigation ist dabei oft fließend.

Empfohlene Maßnahmen

Nicht zuletzt durch Internal Audits werden regelmäßig Betrugsfälle und Verstöße aufgedeckt. Compliance-Fragestellungen werden in der Regel bei jeder Prüfungsplanung berücksichtigt. Verifizieren Sie unter Berücksichtigung bestehender Assurance-Strukturen, wie der Einsatz von Internal Audit zum Thema Compliance für Ihr Unternehmen am effektivsten ist: Als Systemprüfer (z.B. IDW PS 980) oder zur Aufklärung von Hinweisen auf Verstöße oder zur schnellen Beweissicherung bei festgestellten Verstößen. Denkbar ist auch die Beratung bei der Konzeption und Umsetzung von Compliance-Programmen (z.B. bei Whistleblowing-Systemen oder Red-Flag-Analysen) oder die ergänzende Recherche einschlägiger gesetzlicher und regulatorischer Änderungen (Rechtsmonitoring).

Projekt Audit

Strategisch wichtige Projekte erfordern eine klare Projekt-Governance, binden Ressourcen und bergen Risiken bei der Umsetzung. Deshalb sollten erfolgskritische Projekte stets im Internal Audit Universe und in der Prüfungsplanung berücksichtigt sein. Viele Unternehmen sehen sich bei Projekten mit Zeitverzug und/oder Budgetüberschreitungen konfrontiert. Ein professionelles Projektmanagement und eine klare Projekt-Governance sind besonders in komplexen und dynamischen Bereichen von großer Bedeutung. Gerade kapitalintensive Projekte mit verschiedenen Vertragspartnern und Verträgen bergen Kosten- und Ertragsrisiken. Um Einsparungsziele zu identifizieren, wertvolle Einsichten und Empfehlungen zu geben bzw. Prozesse und Kontrollen zu verbessern, sollte Internal Audit Vertragsrisiken und insbesondere Compliance-Aspekte bei seiner Prüfungstätigkeit berücksichtigen. Die meisten erfolgreichen Internal-Audit-Abteilungen verwenden dafür erweitere Tools und Techniken über den gesamten Projekt-Lebenszyklus, um tiefergehende Einblicke und fortlaufende Überwachung zu gewährleisten.

Empfohlene Maßnahmen

Verschaffen Sie sich zunächst einen Überblick über das Projektportfolio und führen Sie eine Risikoeinschätzung durch. Für Projekt-Audits hat der DIIR den Revisionsstandard Nr. 4 herausgegeben. Dabei sollte für die Festlegung des Prüfungsumfangs ein einheitliches Schema möglicher Prüfungsgebiete angewendet werden. Außerdem sind der Status, die Besonderheiten und die Umstände des zu prüfenden Projektes zu berücksichtigen. Ist das Projektmanagement geeignet, um die Projektziele zu erreichen? Sind die Verfahren und Annahmen des Projektantrags plausibel oder sind fachliche Anforderungen im Projekt ordnungsgemäß definiert und umgesetzt? Welche Risiken bzw. Hindernisse existieren, um das Projekt erfolgreich in den Betrieb zu bringen und Mehrwert für das Unternehmen zu schaffen? Entscheidend für den Prüfungserfolg sind Erfahrung und Kompetenz des Prüfers: je nach Prüfungsgebiet (Projektmanagement, Post Merger Integration, Baurevision, Softwareeinführung), Methoden und Tools (z.B. Prüfungsleitfäden, Checklisten, Best-Practices-Standards) sowie Unabhängigkeit des Prüfers.

Leitung Internal Audit

Heinz Wustmann
Partner | Deutschland
hwustmann@deloitte.de

Frank Wehrle
Director | Bereich Süd
fwehrle@deloitte.de

Andreas Langer
Director | Bereich Mitte
anlanger@deloitte.de

Philip Roth
Director | Bereich Nord
philroth@deloitte.de

Andreas Böhner
Director | Bereich Süd/West
aboehner@deloitte.de

Stand 6/2016